Client Security Risk Assessment Questionnaire

Name of Company: Click or tap here to enter text.

Company's Website: Click or tap here to enter text.

Contact Person Completing the Assessment: Click or tap here to enter text.

Email Address: Click or tap here to enter text.

Phone Number: Click or tap here to enter text.

Select the appropriate answer from the drop down in the Response column, and provide a brief description in the Comments section.

		Information Security Assessment Questions	Response	Comments	Endeavor's Comments/Questions to Client responses
		Organizational Information Security			
1		Do you have a member of your organization with dedicated information security duties?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
2		Is a background check required for all employees accessing and handling the organization's data?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
3		Does the organization have written information security policies?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
3.1		If yes, please provide copies when responding to this assessment	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
4		Does the organization have a written password policy that details the required structure of passwords?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.

4.1		How do you verify password strength?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
5		Do all staff receive information security awareness training?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
6		Does the organization have a Data Access Policy and are they willing to comply with the policies as well as the data protection guidelines?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
7		Does the organization have a formal change control process for IT changes?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
8		Will your company be processing credit cards?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
8.1		If yes, is your company PCI DSS compliant?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
General Security					
9		Is antivirus software installed on data processing servers?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
10		Is antivirus software installed on workstations?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
11		Are system and security patches applied to workstations on a routine basis?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
12		Are system and security patches applied to servers on a routine basis?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
12.1		Are system and security patches tested prior to implementation in the production environment?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
13		Do employees have a unique log-in ID when accessing data?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
14		Does the organization have security measures in place for data protection?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
14.1		If yes, please describe in the comments section	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
15		Is access restricted to systems that contain sensitive data? *(credit card numbers, social security numbers, HIPAA, & FERPA data sensitive)*	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.

15.1		If yes, what controls or are currently in place to restrict access?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
16		Is physical access to data processing equipment *(servers and network equipment)* restricted?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
16.1		If yes, what controls are currently in place?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
17		Is there a process for secure disposal of both IT equipment and media?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
17.1		If yes, please describe in the comments section	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
Network Security					
18		Are network boundaries protected by firewalls?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
19		Is regular network vulnerability scanning performed?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
20		Are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) used by your organization?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
20.1		If yes, please describe in the comments section	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
21		Are employees required to use a VPN when accessing the organization's systems from all remote locations?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
22		Is wireless access allowed in your organization?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
22.1		If yes, please describe how it is protected in the comments section	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
Systems Security					
23		Are computer systems *(servers)* backed up according to a regular schedule?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
23.1		Has the back-up and recovery process been verified?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.

23.2		Does the organization store backups offsite?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
23.3		Does the organization encrypt its backups?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
24		Does the organization replicate data to locations outside of the United States?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
25		Does the organization outsource its data storage?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
25.1		If yes, to whom is the data outsourced?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
26		Is there formal control of access to System Administrator privileges?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
27		Are servers configured to capture who accessed a system and what changes were made?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
27.1		If no, in case of a security breach, how do you determine who accessed the system and what changes were made?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
Business Continuity / Disaster Recovery					
28		Does the organization have disaster recovery plans for data processing facilities?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
28.1		What about Business Continuity Plans?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
29		Are computer rooms protected against fire and flood?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
30		Does the organization have a "Hot" recovery site?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
Incident Response					
31		If an information security beach involving sensitive data occurred, what is the defined protocol?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
31.1		If yes, how soon would the Institute be notified?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.

32		Does the organization have a formal Incident Response plan?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
33		Has the organization experienced an information security breach in the past three to five years?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
33.1		If so, please document what information was lost in the comments section?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
33.2		If so, please document how the clients were notified and how quickly in the comments section?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
Auditing / Client Reporting					
34		Does the organization receive an SSAE-16 SOC Report?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
34.1		If so, please document which type of SOC report is being obtained in the comments section. Please provide a copy of the latest SOC report.	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
34.2		If not, does the organization allow clients the right to audit their systems and controls?	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
Additional Security Questions Specific to the Service Offering(s) Provided by the Vendor			**Response**	**Comments**	**Endeavor's Comments/Questions to Client responses**
1		Click or tap here to enter text.	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
2		Click or tap here to enter text.	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.
3		Click or tap here to enter text.	Choose an item.	Click or tap here to enter text.	Click or tap here to enter text.